



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,509	12/12/2003	Sudarshan Palliyil	JP920030270US1	5856
39903	7590	10/17/2007	EXAMINER	
IBM ENDICOTT (ANTHONY ENGLAND)			TURCHEN, JAMES R	
LAW OFFICE OF ANTHONY ENGLAND			ART UNIT	PAPER NUMBER
PO Box 5307			2139	
AUSTIN, TX 78763-5307				
MAIL DATE		DELIVERY MODE		
10/17/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/735,509	PALLIYIL ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 03 August 2007.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 24-44 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 24-44 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
  1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____	6) <input type="checkbox"/> Other: _____

## DETAILED ACTION

Claims 1-23 are cancelled. Claims 24-44 are new.

### *Response to Arguments*

Applicant's arguments with respect to claims 24-44 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 24-44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 24, 31, and 38 recite "detecting whether the as least one changed replica is greater in number than a predetermined number." It is unclear how to compare the changed replica with a predetermined number.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 24-29, 31-36, and 38-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Radatti (US 7,143,113).

Regarding claim 24:

Radatti discloses a method comprising the steps of:

computing first hash values derived from and representing a plurality of replicas of a resource, wherein the replicas are stored on respective data processing systems within a network [*column 3 lines 17-34, the baseline is formed from the master system, all of the subsequent systems are replicas of the master system; therefore hash values derived from a master system represent a plurality of replicas*];

- a) storing the computed first hash values [*column 3 lines 44-48, the secure system data is retained in a storage area, either internally or externally*];
- b) computing current hash values for the replicas of the resource [*column 5 lines 28-34, in the comparison cycle, files are taken one at a time and hashed (MD5)*];
- c) comparing the current and first hash values in order to identify whether all the hash values match [*column 5 lines 33-58, the recent hash is compared with the old hash*];
- d) detecting whether a vulnerability exists responsive to the hash value comparison indicating at least one changed replica of the resource [*column 7 lines 54-58, if an unauthorized user changes the contents, the files modified by the virus will differ*], wherein the detecting comprises:

detecting whether the at least one changed replica is greater in number than a predetermined number [*column 7 lines 54-58, the number of changed files is always greater than zero*]; and

e) presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined number being exceeded [*column 7 lines 24-28, reporting may be used; as is well known in the art it is inherent that the reporting will take place after detection*].

Regarding claim 25:

Radatti discloses the method of claim 24, wherein steps a), b), c), and d) are performed at a first data processing system within the network [*column 3 lines 26-34, the secure system state and secure system data file are generated on the master system; column 6 lines 11-16, the client comparison may take place internally or externally; Radatti also discloses (column 3 lines 8-16) putting an individual computer in "lock down" and scanning for a baseline (in this case a, b, c, and d are performed inside a single computer)*].

Regarding claim 26:

Radatti discloses the method of claim 24, wherein step b) is performed at each replica's respective data processing system, the method further comprising sending the computed hash values to a first data processing system [*column 6 lines 11-16, the hash values can be sent to an external processing system*].

Regarding claim 27:

Radatti discloses the method of claim 24, wherein the vulnerability includes a vulnerability to a computer virus [*column 6 lines 17-38, compared against hashes of viruses*].

Regarding claim 28:

Radatti discloses the method of claim 24, wherein the vulnerability includes a vulnerability to computer hacking [*column 6 lines 17-38, compared against hashes of Trojans and back doors*].

Regarding claim 29:

Radatti discloses the method of claim 24 further comprising:  
classifying as vulnerable the data processing systems storing the replicas,  
wherein the classifying is responsive to the predetermined number or changed replicas  
of the resource being exceeded [*column 9 lines 26-44, dangerous hash values are stored in the dangerous hash value data file, the comparison cycle will then compare new hashes with the dangerous hash file*].

Regarding claims 31-36 and 38-43:

Claims 31-36 and 38-43 are the system and computer program product corresponding to the method claims 24-29 and are rejected under the same reasoning.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 30, 37, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti as applied to claims 24, 31, and 38 above, and further in view of A Distributed Approach against Computer Viruses Inspired by the Immune System hereafter Immune System.

Radatti discloses the method of claim 24, the steps further comprising:  
selecting a sequence of vulnerability-resolution instructions relevant to the vulnerability [column 7 lines 59-65, *the infected files may be restored to a known good state*].

Radatti does not disclose sending a notification of the vulnerability to each data processing system storing one of the replicas and sending the selected instructions to each of the data processing systems storing one of the replicas. Immune System teaches sending a notification of infection to other computers on the LAN to inform them of possible computer viruses (Page 912 – Section 3.3). Each computer in the LAN is programmed to scan its own file upon receiving notification of infection from another computer (Page 912 – Section 3.3). It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Radatti with the notification system of Immune System in order to notify the other computers in the network (Section 3.3.). Radatti or Immune System do not disclose sending selected instructions to each of the data processing systems storing one of the replicas, however, Radatti and Immune system are pre-programmed to handle the situation in which a notification of virus infection has occurred on another computer, then the two will scan their own files to ensure they are virus free. Sending instructions to a computer is well known in the

Art Unit: 2139

art (JAVA, distributed processing systems, remote access and various other client-server models) and it would have been obvious to one of ordinary skill in the art to allow instructions to be received via the network instead of being pre-programmed in order to facilitate a more flexible reaction system to viruses and network intrusions.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

CHRISTOPHER REVAK  
PRIMARY EXAMINER  
